平成 23 年 12 月 1 日

各　位

会　社　名　　ラックホールディングス株式会社
代 表 者 名　　代表取締役社長　　米田　光伸
（JASDAQ・コード番号：３８５７）
問 合 せ 先　　広　報　部　長　　梅田　道幸
電話　０３－６７５７－０１０７

グループ会社のニュース・リリース発信に関するお知らせ

当社子会社の株式会社ラックより「ラック、被害の発覚が相次ぐ「標的型サイバー攻撃・対策支援サービス」を拡充」と題したニュース・リリースが発信されましたのでお知らせいたします。

詳細は添付をご覧ください。

以 上

報道関係各位

2011 年 12 月 1 日
株式会社ラック

ラック、被害の発覚が相次ぐ「標的型サイバー攻撃・対策支援サービス」を拡充
～被害の早期発見と攻撃からの防御、社員教育までをカバーする支援プランを提案～

株式会社ラック（本社：東京都千代田区、代表取締役社長：齋藤　理、以下ラック）は、相次ぐ企業や政府機関への標的型サイバー攻撃に対して、被害の早期発見、防御、教育を支援する、「標的型サイバー攻撃・対策支援サービス」を拡充し、本日 12 月 1 日より提供を開始します。

標的型サイバー攻撃は、特定の組織・企業、個人を狙った犯罪行為です。特定した相手に対して巧妙なメールなどを使い、不正なプログラムを送りつけ、その後潜伏するスパイプログラムに命令を出すことで機密情報などを窃取します。従来のコンピュータウイルスは、不特定多数を狙い、多くの方が被害を受けるかわりに、早期発見と対処ができました。それに対し、相手を特定した標的型攻撃では、知人を装うなど狡猾な詐欺的手口を使って侵入してくるため、攻撃を受けた本人自身が認知する以外に知るすべはなく、被害の発見は難しくなっています。侵入後はホームページを閲覧する普通のネットワーク通信を用いてスパイ活動を行うことなどから、従来の技術的な対策だけでは防御することが困難です。

ラックが対応したセキュリティ事故においても、2008 年に標的型サイバー攻撃と思われる被害が確認され、2011 年に入りこの攻撃が原因で引き起こされたセキュリティ事故が前年対比 2 倍以上に増加しています。これらの標的型サイバー攻撃に対しては、事故を未然に防ぐことは難しく、事故前提に被害を拡大させないよう複数の対策を柔軟に組み合わせたセキュリティ対策が重要です。

◆標的型サイバー攻撃・対策支援サービス概要

この度ラックは、国内最多の情報セキュリティ事故対応の実績から、以下の 3 つのステップで、標的型サイバー攻撃・対策支援サービスを提供します。

サービス分類（＊1）	対策概要	実施期間	概算費用
Step 1. **現状確認による被害の早期発見**	不正侵入の痕跡を確認	約 1 週間	150 万円～
	ネットワーク上での情報漏えい被害を発見	約 1 週間	150 万円～
	チェックリストと確認手順書による自己確認	―	―
Step 2. **出入口の監視による防御**	ウイルスの外部通信を発見し遮断	―	370 万円～（＊2）
	アプリケーション毎に、不正な挙動を発見・遮断	約 1 週間	応相談（＊3）
Step 3. **予防訓練による社員教育**	標的型メール攻撃に対する予防訓練	約 2 ヶ月	150 万円 @100 名

＊1：本サービスは、個別サービスの提供もできます。　　＊2：セキュリティ監視サービスの年間費用です。
＊3：次世代ファイアウォールが出力情報を分析するサービスを提供します。

ラックでは、狡猾な標的型サイバー攻撃によるスパイ行動に対し、政府の防衛活動への協力や被害企業の救済活動を通し、政府組織・企業・個人の資産を守るための支援を行います。本サービスの初年度販売目標は 30 社です。

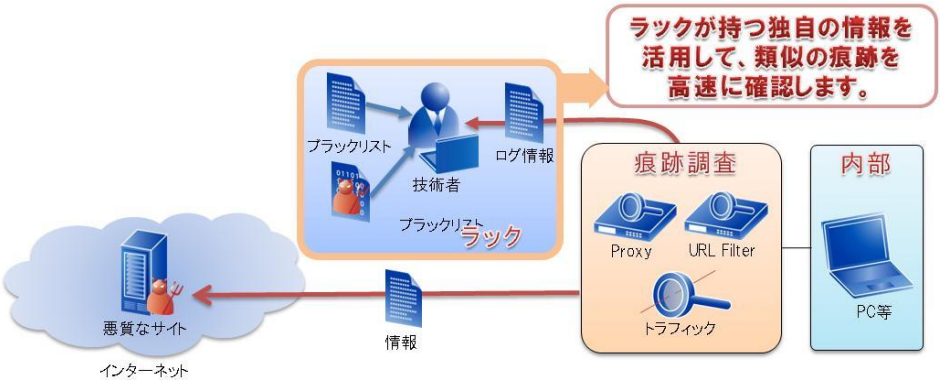
以上

（サービスの概要）

Step 1. 現状確認による被害の早期発見

- 不正侵入の痕跡を確認するログ確認サービス

  プロキシ、URL フィルタリング、ネットワークトラフィックなどのログから、弊社のブラックリストに登録されている IP アドレスにアクセスしていないかを確認し、ウイルスに感染している可能性のある端末を発見します。ブラックリストに登録されていない IP アドレスへの接続についても、送信内容を分析しウイルス感染が懸念される端末を発見します。

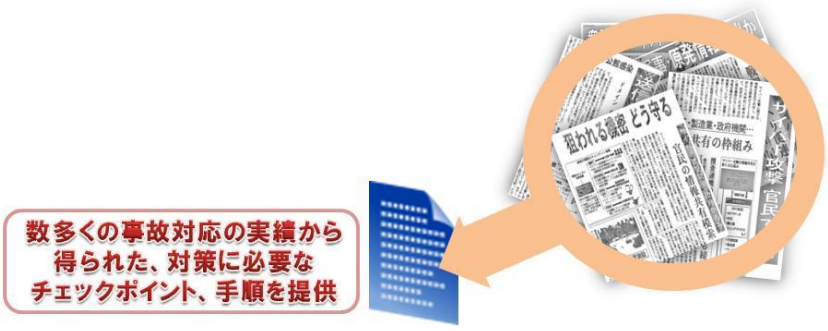


- ネットワーク上の通信を解析する、情報漏えいチェックサービス

  インターネットゲートウェイにラック指定の機材を設置し、収集情報を解析することにより、意図的な外部への情報流出、パソコンのウイルス感染などによる情報漏えい、組織内からの不審なアクセスの有無などを発見します。

- 自己確認用のチェックリストや手順書を提供するサービス

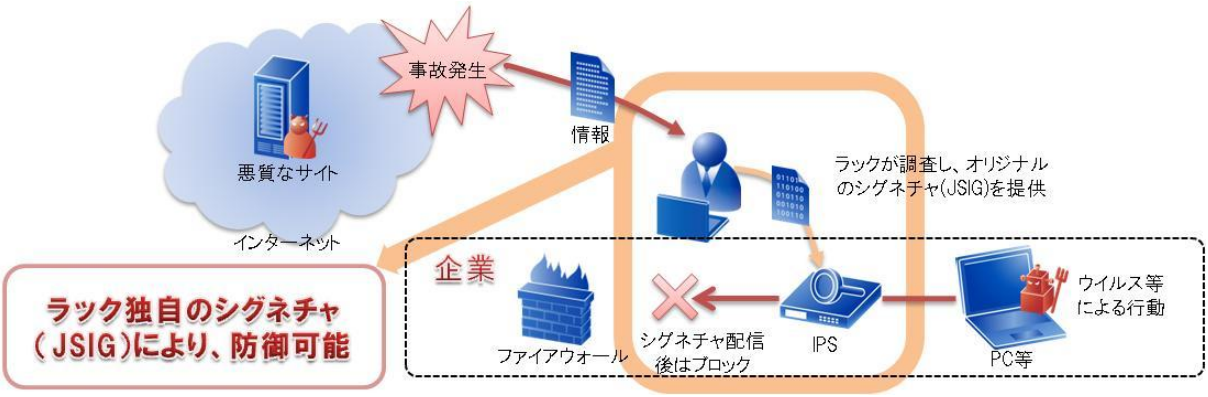
  過去にラックが対応した事案で確認されている被害の痕跡や、ウイルスなどの解析結果から作成された情報から、チェックリストおよび確認手順書を作成しています。この情報を使用して、社内のコンピュータが同様の手口で攻撃を受けていないかを確認することができます。

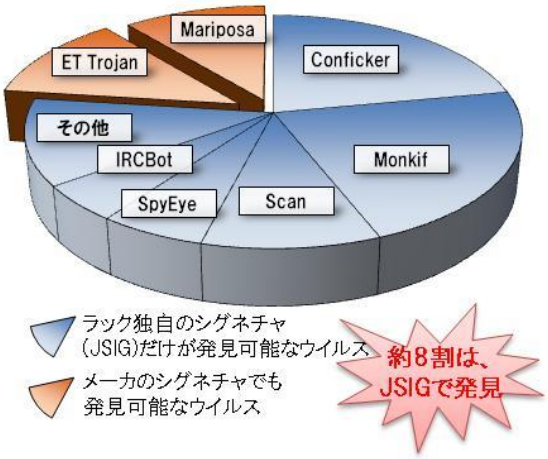


Step 2. 出入口の監視による防御

- ウイルスなどの外部通信を発見し遮断

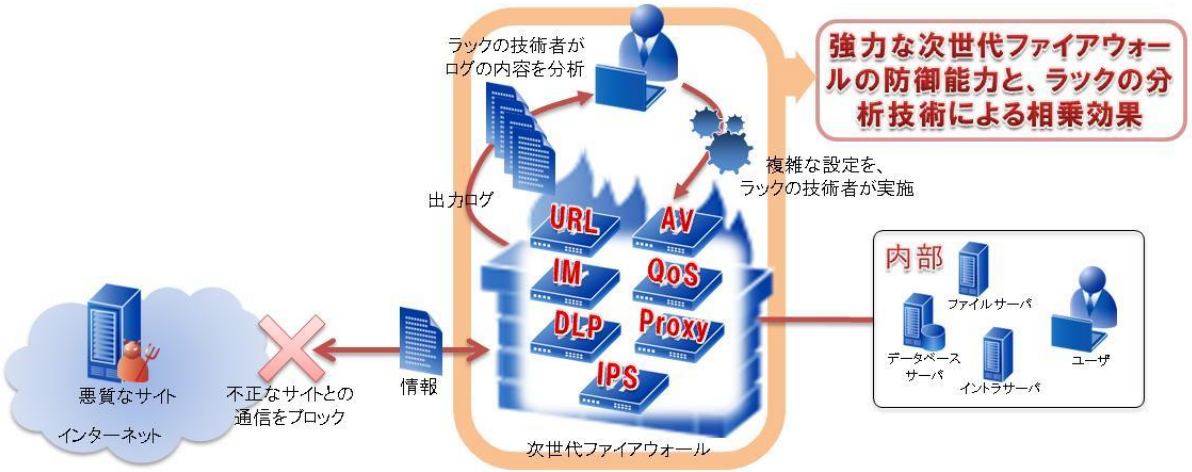
  ネットワーク境界に IPS を設置し、24 時間 365 日の常時監視を提供します。ラックが把握する攻撃手法を、ラック独自の IPS シグネチャとして配信し、メーカシグネチャでは見つからなかった事故を発見します。





- アプリケーション毎に、不正な挙動を発見・遮断

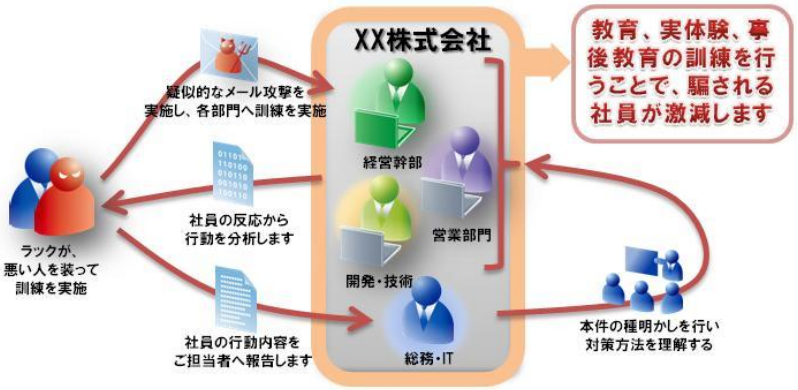
  アプリケーション（FTP/HTTP/HTTPS/IMAP/POP3/SMB/SMTP）レベルでプロトコル解析および制御可能な次世代ファイアウォールを使用して、ネットワーク上のイベントを収集します。大量に収集されるログ情報から、悪影響のあるトラフィックをラックの技術者が分析・発見します。

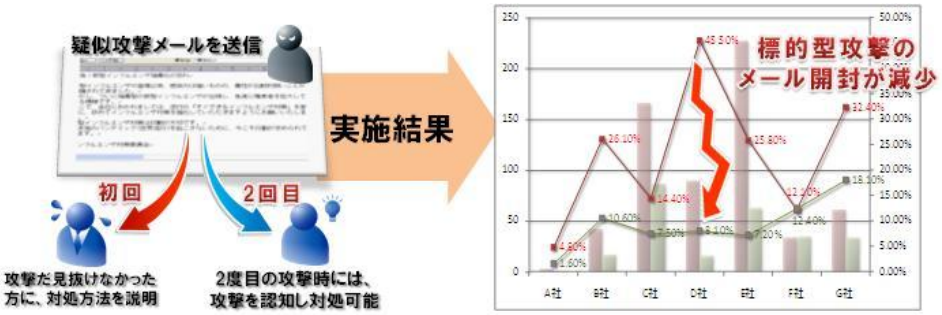


Step 3. **予防訓練による社員教育**

- 標的型メール攻撃に対する予防訓練

  疑似攻撃メールに添付されたファイルを開くか否か、仮に開いてしまった場合にポリシーどおりの行動（上長や専門部署への報告や事後対応など）が行えるかを確認します。 また、標的型のメール攻撃を体験することにより、メールの運用を慎重に行う社員が育成できます。

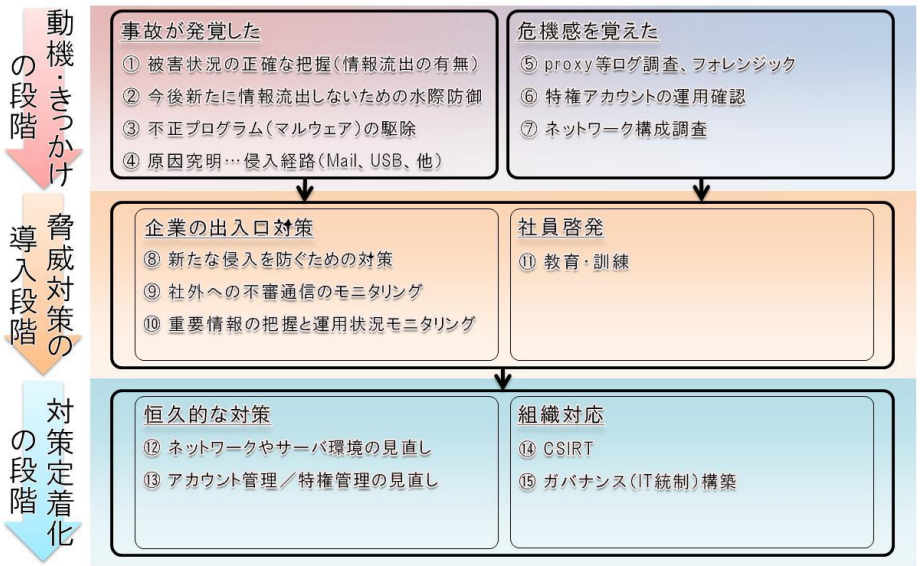




標的型サイバー攻撃に対するさらなる支援

ラックは、標的型サイバー攻撃に対して、以下のようなコンサルティングメニューも用意しています。

ラックのコンサルタントがお客様の要望を伺い、お客様のニーズに合わせた対策を提案させていただきます。



関連リンク

標的型サイバー攻撃に関する 3 ステップ

http://www.lac.co.jp/consulting/tgtattack.html

【株式会社ラックについて】

株式会社ラックは、情報化社会の進展で地球が加速度的に縮小していくことを予測して 1986 年 9 月 3 日に設立されました。セキュリティソリューション分野でのリーディングカンパニーとして、1995 年より提供する「脆弱性診断サービス」、国内最大級の「セキュリティ監視センターJSOC」による 24 時間 365 日の高度な セキュリティ監視・分析サービスの提供、「サイバー救急センター」による情報漏えい事故などの緊急対応・支援など、官公庁・企業・団体等のお客様に総合的なセキュリティソリューションサービスを提供しています。また、ラック ホールディングスグループを挙げて、サイバー社会の安全に貢献してまいります。

【お客様からのお問い合わせ先】

株式会社ラック　営業担当

Tel: 03-6757-0113　E-mail: sales@lac.co.jp

※ 以下のページからもお問い合わせいただけます。

http://www.lac.co.jp/contactus.html

【報道機関からのお問い合わせ先】

株式会社ラック　広報担当

Tel: 03-6757-0130　E-mail: pr@lac.co.jp

*LAC、ラック、JSOC（ジェイソック）は、株式会社ラックの登録商標です。

その他、記載されている製品名、社名は各社の商標または登録商標です。